Deutscher Bundestag **Drucksache 17/8145**

17. Wahlperiode 13. 12. 2011

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Ulla Jelpke, Dr. Petra Sitte, Frank Tempel, Alexander Ulrich, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.

Polizeiliche Soft- und Hardware bei den EU-Agenturen

Seit Jahren rüsten auch polizeiliche EU-Agenturen ihr digitales Arsenal auf. Europol (Europäisches Polizeiamt) will zum „weltweit herausragenden Zentrum der Weltklasse" (world-class centre of excellence) werden, was sich vor allem auf den IT-Bereich bezieht (www.europol.europa.eu/sites/default/files/publications/anniversary_publication.pdf). Zentraler Bestandteil von Europol sind die umfangreichen Datenbanken, deren Einrichtung im Europol-Übereinkommen festgelegt ist. Das „automatisierte System" besteht aus drei Säulen, dem Informationssystem, den Analysedateien und einem Indexsystem. Etliche EU-weite Abkommen erweitern die Zugriffsmöglichkeiten der Behörde. Europol selbst bezeichnet sich als „Information-Broker" und sieht sich dem Grundsatz eines „proaktiven Handelns". Mit dem deutschen Jürgen Storbeck als ersten amtierenden Direktor 1999 und seinem Nachfolger Max-Peter Ratzel, vorher Abteilungspräsident des Bundeskriminalamts (BKA), konnte Deutschland bis zum Antritt des britischen Rob Wainwright 2009 sein Gewicht in der Organisation ausbauen. Max-Peter Ratzel hatte im Oktober 2007 die neue „Strategy for Europol" vorgestellt. Durch die Ausweitung analytischer Kapazitäten sollte die Behörde zum Pionier des „Wandels, Identifizierung und Antwort auf neue Bedrohungen und der Entwicklung neuer Technik" werden. Auch bei Europol kommt Software zur Vorgangsverwaltung, zu Ermittlungs- oder Analysezwecken oder zum Data-Mining zur Anwendung. Nicht nur der Abgleich mehrerer Datensätze ist dabei problematisch und kann als „Profiling" bezeichnet werden. Die Software kann zudem mit „Zusatzapplikationen" oder „Modulen" erweitert werden, um weitere Datenbanken oder das Internet über Schnittstellen einzubinden. Im jüngsten Europol Review wirbt die Agentur mit einer „state-of-the-art facility to extract and analyse crime-related information from digitised data". Unter deutscher Federführung arbeitet bei Europol ein „Mobile Competence Team" (MCT) unter anderem zur Umsetzung des Vertrags von Prüm zum grenzüberschreitenden Datentausch.

Eines der „Angebote" der Agentur ist das „24/7 operational centre", das Daten aus gemeinsamen Operationen von Polizeien der Mitgliedstaaten der Europäischen Union (EU) mit anderen Datensätzen abgleicht (incoming data are quickly cross-checked against all existing data). Die mobile Einheit errichtet eine „live connection" zur Agentur. Genutzt wird die Plattform anscheinend auch für politische Proteste oder Sportereignisse (internationally prominent sporting, economic, political or cultural gatherings). Zur Analyse von Netzwerken nutzt Europol ein „SNA tool", das angeblich bei einer einzigen Aktion (Operation Most) 25 Verdächtige aus einer Million von polnischen Behörden mitgeschnittenen Telefongespräche präsentierte. Europol verfügt außerdem über weitere „forensische Ausrüstung", etwa das „forensic toolkit" (UFED) oder „mobile phone scan-

ners“. Als bewegliche Einheit fungiert ein „expert-operated mobile toolkit for computer data forensics“. Zudem koordiniert Europol ein „Computer Forensic Network“. Bislang unbekannte Methoden und Anwendungen werden innerhalb einer „Cross-Border Surveillance Working Group“ (CSW) erörtert, deren Mitglied Europol ist.

Auch die Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen FRONTEX stattet seine Zentrale in Warschau mit Soft- und Hardware aus. FRONTEX betreibt eine „Situation Center Unit“, um „Risikoanalysen“ oder Lageberichte zu verfassen. Als Nutzeroberfläche entwickelte die Agentur das Frontex One-Stop-Shop web portal (FOSS), an das zunehmend Behörden der EU-Mitgliedstaaten angeschlossen werden und das später das EU-weite Überwachungssystem EUROSUR (Europäisches Grenzkontrollsystem) verwaltet. Weitere digitale Plattformen sind ein „Frontex Media Monitor“ oder die „Joint Operations Reporting Application” (JORA). Hinzu kommen zahlreiche weitere Datenbanken oder Netzwerke, die zunehmend mit digitaler Analysekapazität aufgerüstet werden. Ein „European Network of Law Enforcement Technology Services“ (ENLETS) soll den Erfahrungsaustausch zu digitaler Überwachung EU-weit verbessern und ein Register zu „Sicherheitstechnologie“ anlegen.

Über die Funktionsweise der beschriebenen Anwendungen ist wenig bekannt. Es besteht die Möglichkeit, über den Sachverstand, aber auch die technische Ausrüstung von EU-Agenturen, bestehende nationale Beschränkungen zu umgehen. Die Geschwindigkeit, mit der etwa Europol zum führenden IT-Dienstleister in der Kriminaltechnik avanciert, steht in keinem Verhältnis zur öffentlichen Debatte, inwieweit diese Entwicklung von der Bevölkerung akzeptiert wird. Die digitale Aufrüstung ist nicht verhältnismäßig. Auch ihre Notwendigkeit kann nicht bewiesen werden. Es profitieren indes die großen Rüstungs- und Softwarekonzerne. Wirtschaftliche Argumente zur Ausweitung digitaler Kriminaltechnik, etwa das Einsparen von Beamtinnen und Beamten, führen zur Aushöhlung von Bürger- und Bürgerinnenrechten. Bürgerrechtlerinnen und Bürgerrechtler, netzpolitische Aktivistinnen und Aktivisten, Anwältinnen und Anwälte, soziale Bewegungen und Parlamentarierinnen bzw. Parlamentarier müssen einen Einblick in die Funktionsweise der Anwendungen erlangen. Das Konzept einer informationstechnischen „Überlegenheit auf allen Ebenen“ ist dem Militär entlehnt. Die zunehmend „vorausschauende“ digitale Überwachung setzt die Unschuldsvermutung außer Kraft. Risikoanalysen geraten zum Profiling, wenn auf mehrere Datensätze zugegriffen werden kann. Dieser Prozess ist zudem auf Wachstum angelegt: Statistische Verfahren in der Polizeiarbeit sind auf stets erweiterte und erneuerte Datensätze angewiesen, um „Prognosen“ zu verbessern.

Wir fragen die Bundesregierung:

1. Welche computergestützten Analysewerkzeuge kommen bei welchen Abteilungen der EU-Polizeiagentur Europol zum Einsatz?
   a) Auf welcher Hardware welcher Firmen basieren die Informationssysteme der EU-Agentur (auch Serversysteme und Netzwerke)?
   b) Welche Software welcher Hersteller kommt für welche Bereiche zum Einsatz als
      aa) Vorgangsverwaltung,
      bb) Ermittlungssoftware,
      cc) Analysesoftware,
      dd) Data-Mining,
      ee) Bildersuche?

c) Mit welchen „Zusatzapplikationen“ oder „Modulen“ ist die Software ausgestattet, um etwa weitere Datenbanken oder das Internet über Schnittstellen einzubinden?

d) Welche weiteren Zusatzmodule können für die Software erworben werden, und welche Überlegungen finden hierzu statt?

e) Auf welche Datenbanken können welche Anwendungen im Einzel- und im Regelfall jeweils zugreifen?

2. Welche technischen Kapazitäten im Bereich von Telekommunikationsüberwachung werden vom „24/7 operational centre“ der EU-Agentur Europol entwickelt und angeboten?

a) Nach welchen technischen Verfahren können im „24/7 operational centre“ eingehende Daten aus gemeinsamen Operationen von Polizeien der EU-Mitgliedstaaten mit anderen Datensätzen abgeglichen werden (incoming data are quickly cross-checked against all existing data)?

b) Welche Datenbanken der EU-Agentur oder andere Datensammlungen können derart abgefragt werden, und wie ist dies rechtlich geregelt?

c) Wie und wohin werden gefundene „Treffer“ ausgegeben?

d) Auf welche Weise wird ein weitergehender Bericht (one analytical report) für derartige Operationen ausgefertigt, bzw. welche Daten liegen diesem zugrunde?

e) Welche Rolle spielt das „24/7 operational centre“ in der Koordination „polizeilicher Großlagen“ bzw. welche Überlegungen werden hierzu angestellt?

3. Wie wird die „live connection“ technisch umgesetzt, die Europol im Rahmen seines „24/7 operational centres“ für grenzüberschreitende Operationen anbietet?

a) Welche Hard- und Software welcher Hersteller kommt für dieses „Europol mobile office“ zum Einsatz?

b) Über wie viele „mobile offices“ verfügt Europol und wo sind diese in der Regel „stationiert“?

c) Nach welchen technischen Verfahren und Sicherheitsstandards werden Daten eines „mobile office“ übertragen?

d) Welche Kosten sind für die Ausrüstung von „mobile offices“ entstanden?

e) Worin besteht die Aufgabe der Europol-Bediensteten für die konkrete Handhabung dieses „mobile offices“?

f) Welche konkreten „vast improvements to its mobile office solution“ hat Europol wie im Review 2010 angegeben vorgenommen, die demnach eine „far greater flexibility and speed of deployment“ erlauben würden?

4. Welche Rolle spielt die „powerful mobile office solution“ in der Koordination „polizeilicher Großlagen“?

a) Welche Ereignisse im Bereich „internationally prominent sporting, economic, political or cultural gatherings“ wurden von Europol in den letzten fünf Jahren derart unterstützt, und worin bestand dessen Beitrag?

b) Auf welche Art und Weise arbeitet Europol hinsichtlich von „mobile offices“ mit Verfolgungsbehörden in Rumänien zusammen?

c) Welche Datenbanken und andere „technical equipment“ wurden hierfür in Rumänien installiert?

d) Wie ist die technische Ausrüstung eingebunden in andere internationale Kooperationsprojekte mit Rumänien, darunter auch die Southeast European Cooperative Initiative (SECI) bzw. das Southeast European Law Enforcement Center (SELEC)?

5. Welche Hard- und Software welcher Firmen nutzt das von Deutschland bei Europol ins Leben gerufenen Mobile Competence Team (MCT) unter anderem zur Umsetzung des Vertrags von Prüm zum grenzüberschreitenden Datentausch, und wie wurde deren Beschaffung abgewickelt?

   Worin besteht die Aufgabe des BKA sowie Rumänien und Österreichs innerhalb des MCT hinsichtlich der Nutzung von Soft- und Hardware, etwa als „Testplattform“ für „Pilottests“?

6. Über welche weitere „forensische Ausrüstung“ verfügt Europol, wie im Review 2010 angegeben?

   a) Woraus besteht das im Europol-Review 2010 angeführte „forensic toolkit“ (UFED)?

   b) Wie viele „mobile phone scanners“ bevorratet die EU-Agentur, und um welche Produkte welcher Hersteller handelt es sich?

   c) Nach welchen Kriterien kommen die „mobile phone scanners“ zum Einsatz?

   d) Wie oft und in welchen Ländern wurden die „mobile phone scanners“ von Europol bereits genutzt?

   e) An welchen gemeinsamen Operationen haben deutsche Behörden teilgenommen, innerhalb derer „mobile phone scanners“ von Europol eingesetzt wurden?

7. Welches Werkzeug zur Analyse Sozialer Netzwerke (SNA tool), welcher Hersteller ist von Europol konkret gemeint, das bei der „Operation Most“ zum Einsatz kam?

   a) Über welche Funktionalitäten verfügt dieses „SNA tool“, und welche mathematischen Algorithmen kommen dabei zur Anwendung?

   b) Auf welche Datenbanken greift das „SNA tool“ im Regel- und im Einzelfall zu?

   c) Auf welche Art und Weise hat das „SNA tool“ bei der „Operation Most“ dafür gesorgt, 25 Verdächtige aus einer Million mitgeschnittenen Telefongesprächen zu extrahieren?

   d) Wie ist die Funktionsfähigkeit dieses „SNA tools“ getestet worden?

   e) Welche anderen Anbieter ähnlicher Software wurden vor oder nach der Einführung des „SNA tools“ hinsichtlich einer Verbesserung, Evaluierung oder Anschaffung anderer Produkte eingebunden?

   f) Wie wird sichergestellt, dass die aufgrund der Analyse des „SNA tools“ Verhafteten nicht durch einen Softwarefehler ins Visier der festnehmenden Behörden in Polen gerieten?

   g) Wie wird sichergestellt, dass die derart erlangten Erkenntnisse vor Gericht verwertet werden können?

   h) Wie oft wurde das „SNA tool“ von Europol bereits eingesetzt, und bei welchen Operationen waren Behörden der Bundesregierung daran beteiligt?

   i) In welchen internationalen Arbeitsgruppen erörtert Europol operative oder technische Aspekte hinsichtlich des Einsatzes von „SNA tools“?

8. Auf welche deutschen Informationssysteme haben die Agenturen Europol und Eurojust (Einheit für justizielle Zusammenarbeit der Europäischen Union – EUROJUST) lesenden oder schreibenden Zugriff?

   a) Wie ist geregelt, inwieweit die hierüber erlangten Informationen mit forensischen Methoden Europols ausgewertet werden dürfen?

   b) Wie wird ausgeschlossen, dass die Daten ohne Wissen deutscher Behörden in Ermittlungen von Europol verwendet werden?

   c) Welchen Inhalt hatte das „Proposal on Social Media Communication guidelines for law enforcement authorities“, das von der früheren ungarischen Ratspräsidentschaft vorgestellt wurde?

9. Worin besteht die Aufgabe des „Computer Forensic Networks“ bei Europol?

   a) Welche Anwendung ist gemeint, die Europol im Review 2010 mit „state-of-the-art facility to extract and analyse crime-related information from digitised data“ bewirbt?

   b) Welche Produkte welcher Hersteller werden hierfür eingesetzt?

   c) Wie hat Europol bewerkstelligt, „dramatic improvements in the quantity of data that can be processed“ vorzunehmen?

   d) Worin besteht das „expert-operated mobile toolkit for computer data forensics“, und über welche Funktionalitäten verfügt die Anwendung?

10. Worin besteht die Arbeit der „Cross-Border Surveillance Working Group“ (CSW), deren Mitglied Europol ist?

    a) Seit wann existiert die CSW, und welche Behörden oder sonstigen Stellen welcher Länder nehmen daran teil?

    b) Auf wessen Veranlassung wurde die Gruppe gegründet?

    c) Welche Themen bzw. konkreten Überwachungswerkzeuge standen auf den Treffen der letzten fünf Jahre jeweils auf der Tagesordnung?

    d) Welche Methoden zur verdeckten Beobachtung von Personen oder Sachen hat Europol entwickelt bzw. setzt diese ein?

11. Welche Soft- und Hardware welcher Hersteller wird von der EU-Agentur FRONTEX (etwa zur Fallbearbeitung) eingesetzt und wie wurde ihre Beschaffung geregelt?

    a) Welche Software welcher Hersteller wird von der „Frontex Situation Center Unit“ genutzt, um „Risikoanalysen“ oder Lageberichte zu verfassen?

    b) Welche Software welcher Hersteller liegt dem „Frontex One-Stop-Shop web portal“ (FOSS) zugrunde?

    c) Welche Behörden der EU-Mitgliedstaaten sind bereits an das FOSS angebunden bzw. sollen zukünftig angeschlossen werden?

    d) Welche Software welcher Hersteller liegen dem „Frontex Media Monitor“ zugrunde und welche technische Spezifikationen erfüllt die Anwendung?

    e) Auf welcher Software welcher Hersteller basiert die „Joint Operations Reporting Application“ (JORA), und welche technische Spezifikationen erfüllt die Anwendung?

    f) Wie sind Schreib- und Leserechte für beteiligte Stellen und Behörden der Mitgliedstaaten innerhalb des FOSS, des „Frontex Media Monitors“ und des JORA geregelt?

12. Welche Überlegungen wurden von der Bundesregierung bislang zur Beteiligung am „Common Pre-Frontier Intelligence Picture“ (CPIP) angestellt, mit dem der „vorgelagerte Grenzbereich“ innerhalb von EUROSUR überwacht werden soll?

    a) Wo könnte ein deutsches „National Coordination Centre“ (NCC) im Rahmen von EUROSUR angesiedelt werden, und welche Überlegungen wurden hierzu von wem bereits angestellt?

    b) Welche Aufgaben würde ein deutsches NCC übernehmen?

13. Inwieweit nutzt Deutschland hinsichtlich des „Europäischen Strafregisterinformationssystems“ (ECRIS) Anwendungen der „Interactive Listening and CONNecting“ (iLiCONN), und um welche Soft- und Hardware welcher Hersteller handelt es sich dabei konkret?

    a) Auf welche Datenbanken greift iLiCONN zu, bzw. welche sonstigen Datensätze werden verarbeitet?

    b) Wie wurde die Anwendung zuvor getestet, und welche Kriterien zur Qualitätssicherungen mussten erfüllt werden?

    c) Haben deutsche Behörden die Möglichkeit, den Quellcode verwendeter Software einzusehen oder anderweitig zu prüfen?

14. Inwieweit ist das „European Network of Law Enforcement Technology Services“ (ENLETS) mit der Durchführung, Erörterung oder Evaluierung von Maßnahmen zur Kommunikationsüberwachung befasst?

    a) Welche Treffen mit welchen Inhalten haben seit Gründung des ENLETS stattgefunden?

    b) Welche Technologien werden derzeit innerhalb von ENLETS behandelt?

    c) Welche Angaben macht die Bundesregierung hinsichtlich des Registers zu „Sicherheitstechnologie“, das innerhalb von ENLETS angelegt werden soll?

    d) Welche Stelle wird von deutschen Behörden als „ENLETS National Contact Point“ benannt?

    e) Wie arbeiten andere EU-Agenturen innerhalb von ENLETS mit?

    f) Mit welchen Kapazitäten vor allem im IT-Bereich arbeitet die Polizeiagentur Europol in ENLETS mit?

    g) Inwieweit sind Firmen der Rüstungs- und Softwareindustrie in die Arbeit von ENLETS eingebunden?

    h) Welche Zusammenarbeit pflegt ENLETS mit Instituten, Hochschulen oder sonstigen Einrichtungen der EU-Mitgliedstaaten?

    i) Inwieweit berücksichtigt ENLETS laufende EU-Forschungsvorhaben im Bereich der Sicherheits- und Überwachungstechnik?

    j) Was wurde anlässlich des Vortrags von dem Wissenschaftler Andrzej Dziech von der AGH University of Science and Technology in Krakau (Polen) bei einem der jüngsten Treffen von ENLETS besprochen, und welche weiteren Verabredungen wurden getroffen?

Berlin, den 13. Dezember 2011

Dr. Gregor Gysi und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333